IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF THE SILVER HP LAPTOP BEARING SERIAL NUMBER 5CD123DYX3 AND ASSOCIATED WITH VICTOR ORTIZ	Magistrate No. 23-mj-2198

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A SEARCH WARRANT

I, Francisco J. Zayas, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – an electronic device – which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent employed by the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations ("HSI"), assigned to the Office of the Special Agent in Charge, Philadelphia, Pennsylvania. I have been employed in such capacity since April 2021. Prior to becoming a Special Agent with HSI, I was a Police Officer for the City of Philadelphia for approximately eight years. In February 2022, I completed the Federal Law Enforcement Criminal Investigator Training Program as well as the Immigration and Customs Enforcement Special Agent Training Academy located in Glynco, Georgia. As an HSI Special Agent, I have experience conducting criminal investigations as it pertains to violations of federal law. I was previously assigned to the HSI Philadelphia National Security group and I am currently assigned to the HSI Philadelphia Liberty Border Enforcement Security Taskforce (BEST) group. I have investigated and assisted with the investigation of numerous cases involving but not limited to firearms violations, war crimes, human rights

violations, human smuggling, and drug trafficking. I have extensive training and experience conducting and assisting with criminal investigations including, but not limited to, the instant case.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, law enforcement officers and witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is the silver HP laptop bearing serial number 5CD123DYX3 and seized from the residence of Victor ORTIZ (hereinafter, the "Device").

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

May 4, 2022 Assault

6. On May 4, 2022, while Victim 1[1] was walking to work, an assailant, later identified as Victor ORTIZ, threw a caustic substance at Victim 1 near her office at 30 North 41st Street in Philadelphia, Pennsylvania. Based on interviews of Victim 1, recovered

[1] Victim 1, who was a federal employee on the date of the attack, is a person that is known to, and has been interviewed by, law enforcement in connection with this investigation. Victim 1 provided information to law enforcement as a victim in this case and not in expectation of receiving financial compensation or prosecutorial or judicial consideration. Victim 1 is believed to be truthful and credible as aspects of the information have been independently corroborated by this investigation.

surveillance video, and police reports, I believe the assault took place at approximately 7:00 a.m. The assailant took Victim 1's cell phone during the attack.

7. Following the attack, Victim 1 was transported to Penn Presbyterian Hospital, where she was treated for chemical burns to her body and face, as well as burns and abrasions on her cornea.

8. Philadelphia Police Department ("PPD") Detectives interviewed Victim 1 at Penn Presbyterian Hospital on the day of the assault, and she stated that the attacker came up from behind her and threw liquid in her face. She described the attacker as a 5'6" black or Hispanic male with a light complexion, black clothing, and a mask. This description is consistent with ORTIZ's physical appearance in that he is a 5'7" Hispanic male with a light complexion. Victim 1 stated she could not open her left eye due to the attack and that her skin was burning. Victim 1 did not identify the attacker. Based on my experience with robberies, this crime was unusual in that the attacker used chemicals to disarm the victim and when he did, he only stole her cell phone and not her wallet, money, or purse.

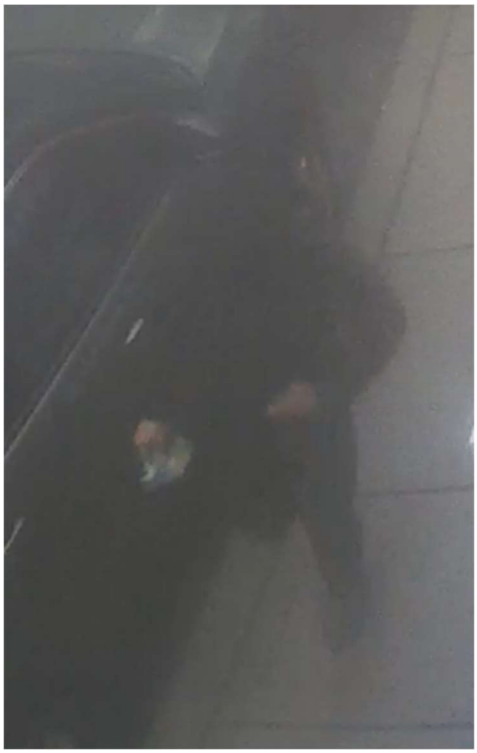
9. Penn Presbyterian Hospital treated Victim 1 for a corneal abrasion, chemical burns of the cornea due to an alkaline substance, and chemical burns of her chest wall. Victim 1 told investigators that she was unable to open her eye for several days and lost more than half of her vison for an extended period. Victim 1 also told investigators that she sustained burn injuries to her ear and chest with painful wounds that persisted for months.

10. On or around May 12, 2022, Philadelphia detectives retrieved security camera footage from a residence near the attack. The security camera footage showed a male wearing dark colored clothing at or around the time of the attack. This male fit the description of the offender provided by Victim 1. The male appeared to be walking in the video. This security

camera footage was shown to Victim 1. Victim 1 told detectives that she did not recognize the individual but agreed that the male matched the description of the offender.

11. On or around May 24, 2022, agents retrieved additional videos from two private residences near where the male assaulted and robbed Victim 1. The first video, obtained from a camera located at a private residence on the 300 block of North Holly Street, shows Victim 1 parking her vehicle and walking towards her office. On the near side of the street, a person wearing all-black clothing and holding an object approaches the victim from behind. The assault occurs outside of the view of the camera. The offender is then seen running back towards where he initially appeared. The second video, obtained from a private residence on the 300 block of North 42nd Street, shows the same offender walking through an alleyway and making a right turn out of view of the camera. The offender's clothing is visible on both videos.

12. On or about June 4, 2022, Victim 1 viewed the surveillance footage that agents gathered. This was the first time Victim 1 had viewed this footage. Victim 1 viewed the footage until the subject was closest to the camera and then stated, "that's Victor." A PPD Detective rewound the footage and paused the video. Again, Victim 1 stated, "that's Victor, that's my ex." The PPD Detective played the footage one frame at a time and Victim 1 stated, "those are his boots, those are his hands, that's him." Victim 1 stated, "I was with him for seven years, I know [that's] him." The below picture is a still image of the video from which Victim 1 identified ORTIZ.



13. In addition to identifying her ex-boyfriend as ORTIZ, Victim 1 provided his cellular phone number as 215-858-3332. Victim 1 further stated that ORTIZ uses a Samsung Galaxy cell phone. Subpoena returns provided by AT&T confirm that ORTIZ is the subscriber to 215-858-3332 and that the associated International Mobile Equipment Identity number is 3550481079393373 Samsung SM G975U, also known as a Samsung Galaxy S10 Plus phone. Victim 1 stated that ORTIZ lives at 2508 North 5th Street in Philadelphia and that he always carries his cell phone with him.

14. On or about May 6, 2022, HSI Philadelphia requested GPS locations of Victim 1's stolen phone via an exigent request to cell provider T-Mobile.

15. On or about June 30, 2022, HSI Philadelphia received results from a forensics laboratory identifying the substance used in the attack. Victim 1 turned over the jacket worn during the attack that was severely stained with the caustic chemical substance. The lab report

indicated that the residue from the submitted jacket contained sodium carbonate hydrate. I know this substance to also be referred to as soda ash, a substance commonly used in industrial cleaning. HSI Philadelphia reached out to an industry professional to inquire about the substance. The owner of a power washing company described soda ash as being commonly used in the industry and stated it could be very dangerous if any contact is made with bare skin. Victim 1 stated, and Pennsylvania state records confirm, that ORTIZ has a power washing company, Ortiz Pro Washing, LLC.

Use of GPS Tracker by ORTIZ

16. Victim 1 told investigators that she believed ORTIZ was tracking her location, utilizing a GPS-enabled device located on or in her vehicle. Victim 1 stated that while they were dating, Victim 1 saw paperwork alleging ORTIZ was formally accused of tracking a prior girlfriend utilizing a GPS-enabled device. Victim 1 further stated that ORTIZ told her that he used a GPS tracking device on an ex-girlfriend and "he used a pre-paid sim card."

17. On or about June 6, 2022, HSI agents inspected two vehicles that Victim 1 drives regularly. HSI agents located a tracking device on a Toyota 4Runner registered to Victim 1's mother. Victim 1 stated ORTIZ knows that Victim 1 often drives the 4Runner. The device was held to the frame of the vehicle by a magnet and appeared to be in a 3" x 4" weatherproof "Pelican-brand" case. I know that devices such as this are utilized by law enforcement and are typically shrouded in weather-proof cases. The device was photographed in place and HSI Philadelphia requested a crime scene unit from the Philadelphia Police Department to process the device for fingerprints and forensic evidence. Upon receiving the information that HSI found a device on her vehicle, Victim 1 became significantly distressed. Victim 1 stated that ORTIZ

previously had unsupervised access to the vehicle for approximately one hour when he offered to replace its brakes.

18. Because there was no crime scene technician available to process the device for forensic evidence prior to removing it from the vehicle, it was not removed. I know through training and experience that devices shrouded in cases can have tamper-evident "photocells" that alert the owner if they are opened, exposing light to the photocell, and that experts are thus required to remove the device in a way that preserves it.

19. On June 7, 2022, law enforcement agents tried to get the device off the car but it was no longer there. Victim 1 stated that she did not remove the device from her vehicle.

20. On July 6, 2022, Victim 1 contacted HSI Special Agents, stating "He [ORTIZ] just drove by my house. My mom saw him and he was waving." The next day, July 7, 2022, Victim 1 contacted HSI Special Agents, stating "Call me when you can. I think he bugged me I have video." HSI Philadelphia accessed video files from Victim 1's "Blink" brand security cameras. The videos were taken at approximately 1:05 a.m. HSI agents reviewed the video and observed an individual on his back, underneath the rear of Victim 1's Toyota Corolla. The second video shows the same individual walking toward Victim 1's Toyota 4runner. The individual is illuminated by a motion light and appears to notice the camera, looking up prior to fleeing. The below picture shows the individual.

21. Victim 1 identified ORTIZ as the individual in the video and the above screenshot. The physical mannerisms of the individual running from Victim 1's residence are similar to the physical mannerisms of the individual running from the scene of the chemical attack on May 4, 2022. HSI Special Agents performed a physical inspection of Victim 1's vehicles and did not find any GPS devices.

22. HSI Philadelphia issued an administrative subpoena to real-time GPS tracking platform "Spytec GPS" for subscriber and customer account information for ORTIZ. On or about August 12, 2022, HSI Philadelphia received returns showing ORTIZ has been a customer of Spytec GPS since January 16, 2020. Returns show ORTIZ subscribed to the service "PU_GL300_MONTHLY_BASIC / monthly $24.95 USD." According to spytec.com/pricing, the subscription package provides "Live Tracking." Payments were processed and settled on

April 20, 2022, May 20, 2022, and June 20, 2022. Payments were processed and declined five times in July and August 2022.

ORTIZ's Laptop

23. On or about July 27, 2022, HSI Philadelphia assisted the Philadelphia Police Department in searching ORTIZ's residence at 2508 North 5th Street in Philadelphia, Pennsylvania, pursuant to a warrant, and arresting him for Pennsylvania crimes. During the search, agents seized a silver HP laptop bearing serial number 5CD123DYX3 which was located in the same bedroom as ORTIZ's Samsung Galaxy 10 cell phone.

Analysis of Cell Phone Location Information

24. On September 21, 2022, the Honorable Richard A. Lloret approved a search warrant for ORTIZ's cell phone location information. The FBI has analyzed the location information for ORTIZ's cell phone and Victim 1's cell phone.

25. On May 4, 2022, at approximately 4:47 a.m., ORTIZ's phone left the vicinity of his home in North Philadelphia and traveled approximately 17 miles to the vicinity of Victim 1's home in Bucks County, Pennsylvania, arriving at approximately 5:21 a.m.

26. At approximately 6:15 a.m., Victim 1's phone and ORTIZ's phone both traveled from the area of her residence to the area of her workplace in West Philadelphia, arriving at approximately 7:00 a.m.

27. Following the attack, both Victim 1's phone and ORTIZ's phone travelled to North Philadelphia and were near ORTIZ's house at approximately 8:00 a.m.

28. On June 6, 2022, ORTIZ's phone was near the location where agents were examining Victim 1's vehicle, at the same time that agents were examining her vehicle and observed the aforementioned Pelican-type case. Victim 1 returned to her home in Bucks County

that afternoon, and Ortiz's phone was subsequently used at or near Victim 1's home. The next day, the Pelican case was no longer on Victim 1's vehicle.

29. Approximately 30 minutes after the picture in paragraph 20 was taken at Victim 1's house on July 7, 2022, Ortiz's phone was used in the vicinity of Victim 1's house.

The Posting of Pictures of Victim 1

30. The phone taken during the assault of Victim 1 contained personal pictures of Victim 1 that were of a sexual nature. On May 25, 2022, these pictures were posted onto Victim 1's Facebook account by an individual other than Victim 1. Victim 1's phone was logged into Facebook at the time it was stolen, and the password of the phone was her birthday. ORTIZ knows the date of Victim 1's birthday.

ORTIZ's Federal Charges

31. A grand jury sitting in the Eastern District of Pennsylvania has returned an indictment charging Victor ORTIZ with the following offenses: 18 U.S.C. § 2261A(2)(A) & (B), 2261(b)(3) (stalking) and 18 U.S.C. § 111(a)(1) & (b) (assault of a federal employee[2]).

TECHNICAL TERMS

32. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178).

[2] Victim 1 is an employee of the United States who was walking to work at the time ORTIZ attacked her.

Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

33. In my training and experience, examining data stored on laptops can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

34. Specifically, based on my training and experience, I know that individuals often connect a cell phone to a laptop to view materials on the phone, download materials from the phone, and/or post those materials onto the Internet. Since pictures from Victim 1's phone were posted onto the Internet, I believe there is probable cause that a search of the Device will show that it was used to access Victim 1's phone, download materials from the phone, and/or post pictures from the phone onto the Internet.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

35. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the

Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

36. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or

application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

37. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

38. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

39. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

40. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

/s/ Francisco J. Zayas
Francisco J. Zayas
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on December 21st, 2023.

/s/ PAMELA A. CARLOS
THE HONORABLE PAMELA A. CARLOS
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

The property to be searched is a silver HP laptop bearing serial number 5CD123DYX3 seized from the residence of Victor ORTIZ (hereinafter, the "Device").

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. § 111(a)(1), assault on a federal employee, and 18 U.S.C. § 2261A(2), stalking, and involve Victor ORTIZ from May 4, 2022, through July 27, 2022 (the date the Device was seized), including:

   a. All records showing that Victim 1's cell phone was accessed by and/or downloaded onto the Device.

   b. All records showing that materials from Victim 1's cell phone were posted onto the Internet by the Device.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.